## REMARKS

Claims 1-30 are currently pending in the subject application and are presently under consideration. Claims 1, 5, 6, 9, 11, 15, 16, 19, 21, 23, 25, 26, and 29 have been amended as shown on pp. 2-8 of the Reply.

Applicants' representative thanks the Examiner for the courtesies extended during the telephonic interview on February 26, 2008, between Examiner Roderick Tolentino and Applicant's representative Bradley Spitz. During the interview, the rejection of claims 1-30 under 35 U.S.C. §103 was discussed. Applicant's representative submitted proposed amendments and related arguments that the art of record does not disclose or suggest the features of (1) initiating registration *via* engagement of a trigger at a first device and acknowledgement of engagement of the trigger at a second device or (2) generation and use of a commitment value as a safeguard in the registration process prior to key generation. It was agreed upon during the interview that the art of record does not disclose or suggest the generation and use of a commitment value; however, no such agreement was reached regarding initiating registration *via* engagement of a trigger.

Accordingly, in the interest of expediting prosecution, Applicant's representative has amended the claims as shown on pp. 2-8 of the Reply to recite the generation and use of a commitment value prior to key generation. It is noted, however, that such amendments are made notwithstanding Applicant's representative's disagreement with the present rejection, and that Applicant's representative reserves the right to pursue the original and/or rejected claims at a later date, *e.g.*, by filing a continuation application.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

## I. Rejection of Claims 1-30 Under 35 U.S.C. §103(a)

Claims 1-30 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Nessett *et al.* (U.S. 6,766,453) in view of Berman *et al.* (U.S. 2003/022116), Dujari *et al.* (U.S. 7,191,467), and Lintulampi (U.S. 6,377,804). Withdrawal of this rejection is requested for at least the following reasons. The cited references, either alone or in combination, do not disclose or suggest all features recited in the subject claims. "To reject claims in an application under §103

. . . the prior art reference (or references when combined) must teach or suggest all the claim limitations." MPEP §2142; s*ee In re Vaeck,* 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

Independent Claims 1, 15, and 25

Independent claim 1 (and its corresponding dependent claims) recites a technique for registering a first device with a second device. The registration process is initiated when a triggering mechanism coupled to the first device is engaged and engagement of the trigger is acknowledged at the second device. (*See* Specification, p. 7, ll. 18-22 and p. 20, ll. 20-23). In addition, "commitment" information is communicated between the registering devices as an additional safeguard in the registration process. More specifically, the first device derives commitment information from a registration nonce or another security value and communicates the commitment information to the second device. Later in the registration process, the first device can communicate a security value to the second device. If the second device cannot correctly derive the commitment information from the security value (which may be the case, for example, if the security value changed during the registration process due to an attack), registration is terminated. (*See* Specification, pp. 17-18 (Protocol Flow 3)).

To the above ends, independent claim 1 recites: *A method for registering a first device with a second device, comprising the steps of:* ***initiating communication between the first device and the second device over a first communication channel by engaging a trigger at the first device and detecting at the second device that the trigger at the first device has been engaged****; upon initiation of communication between the first device and the second device,* ***deriving a commitment value at the first device from a registration nonce value known to the first device and communicating the commitment value from the first device to the second device****; communicating information from the second device to the first device for use in generating a secret;* ***communicating a registration nonce value from the first device to the second device*** *in response to the information communicated from the second device; at the second device,* ***attempting to derive the commitment value from the registration nonce value communicated from the first device; if the commitment value is successfully derived by the second device, generating a first secret*** *known to the first device and a second secret known to the second device using communications between the first device and the second device over the first communication channel; from the first device, producing first information derived from the first*

*secret; from the second device, producing second information derived from the second secret; using a communication channel other than the first communication channel, comparing the first information and the second information in a manner sufficient to assure a third party that the first secret and the second secret are the same; and enabling the first and second device to use the first and second secrets upon the third party being assured that the first secret and the second secret are the same*. The cited references do not disclose or suggest such novel features.

Nessett *et al.* relates to a Diffie-Hellman key agreement protocol that can be utilized by a pair of registering network entities that share respective secret keys with a third party RADIUS server. The registering devices initially generate message authentication codes based on the respective secret keys of the devices and public security information chosen by the devices. The message authentication codes and public security information are then communicated to the RADIUS server, which utilizes the secret keys of the devices and the public security information to verify the message authentication codes. (*See*, *e.g.*, Fig. 3 and col. 7, l. 37 – col. 10, l. 36).

At Page 3 of the Office Action, the Examiner asserts that Nessett *et al.* teaches generating a first secret known to the first device and a second secret known to the second device using communications over a first communication channel and producing information derived from said secrets. However, Nessett *et al.* is silent regarding *initiating communication between a first device and a second device by engaging a trigger at the first device and detecting at the second device that the trigger at the first device has been engaged* and *generation and use of a commitment value* as recited by independent claim 1. As conceded by the Examiner at Page 3 of the Office Action, Nessett *et al.* does not teach the use of a trigger for initializing registration. Further, regarding the generation and use of a commitment value, the verification process disclosed by Nessett *et al.* is performed by a third party RADIUS server instead of a first registering device and a second registering device, as recited by independent claim 1. In addition, Nessett *et al.* discloses that pre-existing knowledge of the secret keys being generated at the RADIUS server is required by the process in Nessett for verification. Applicant's representative submits that requiring such advance knowledge of the secret keys to be generated is contrary to the purpose of requiring the commitment, namely ensuring that devices are only permitted register if the commitment is maintained. In contrast, registering devices undergoing the process disclosed by Nessett *et al.* are required to pre-register with the RADIUS server to allow the RADIUS server to have the keys prior to registration.

At Pages 3-4 of the Office Action, the Examiner relies on Dujari *et al.* and Berman *et al.* to overcome the noted deficiencies of Nessett *et al.* However, Dujari et al., which relates to techniques for authentication between an Internet client and a server *via* a third party authentication service, and Berman *et al.*, which relates to techniques for mutual authentication between a client and a server, are similarly silent regarding *initiating communication between a first device and a second device by engaging a trigger at the first device and detecting at the second device that the trigger at the first device has been engaged* and *generation and use of a commitment value* as recited by independent claim 1.

The Examiner further relies on Lintulampi at Page 4 of the Office Action to overcome the noted deficiencies of Nessett *et al.* with regard to the use of a trigger for initiating registration. Lintulampi relates to techniques by which a mobile terminal can register with a cellular communication network upon requesting a service. As disclosed by Lintulampi, a mobile terminal initially utilizes a GSM or other network as its home network (HPLMN), such that upon requesting a service the service request is received by the home network. The home network can then service the request if it can do so or initiate registration between the terminal and a UMTS or other network if it cannot. (*See*, *e.g.*, col. 3, ll. 52-65; col. 4, ll. 43-65; col. 5, ll. 41-63). At Page 4 of the Office Action, the Examiner asserts that Lintulampi teaches initiating communication between the first device and the second device over a first communication channel by engaging a trigger at the first device and detecting at the second device that the trigger at the first device has been engaged. Applicant's representative respectfully disagrees with this assertion for at least the following reasons. First, Lintulampi discloses that it is a request for a service, and not necessarily an engagement of a physical trigger, that initiates the processes disclosed therein. Second, even if a service request suggests engagement of a physical trigger, which is an assertion with which Applicant's representative does not agree, the service request does not directly trigger registration between a mobile terminal and a mobile network due to the fact that the mobile terminal is pre-registered to a home network prior to the service request. In contrast, it is disclosed by Lintulampi that registration is not triggered in response to a service request if the home network to which the mobile terminal is already registered can service the request.

Independent claims 15 and 25 have been amended in a similar manner to independent claim 1. Accordingly, for at least the reasons stated above, the cited references, either alone or in combination, do not disclose or suggest all features recited by independent claims 1, 15, and 25.

Independent Claims 5 and 11

Independent claims 5 and 11 (and their corresponding dependent claims) have been amended to contain similar limitations to independent claim 1, with the additional limitation that a trigger utilized for initializing registration is a switch or a button. Accordingly, the cited references do not disclose or suggest all claimed features of independent claims 5 and 11 for at least the reasons stated above regarding independent claim 1, with the additional reason that the cited references, either alone or in combination, do not disclose or suggest *initiating registration via engagement of a switch or a button coupled to a registering device.*

Independent Claim 21

Independent claim 21 (and its corresponding dependent claims) has been amended to contain similar limitations to independent claim 1, with the additional limitation that a commitment value is generated by computing a hash of a registration nonce. Accordingly, the cited references do not disclose or suggest all claimed features of independent claim 21 for at least the reasons stated above regarding independent claim 1, with the additional reason that the cited references, either alone or in combination, do not disclose or suggest *deriving a commitment value from a registration nonce by computing a hash of the registration nonce.*

## CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP1996US].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicant's undersigned representative at the telephone number below.

Respectfully submitted,

AMIN, TUROCY & CALVIN, LLP

/Himanshu S. Amin/
Himanshu S. Amin
Reg. No. 40,894

AMIN, TUROCY & CALVIN, LLP
24TH Floor, National City Center
1900 E. 9TH Street
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731